Certification Report

EAL 4+ Evaluation of Sun Microsystems Inc.

Solaris™ 9

Release 8/03

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-26-CR
Version: 1.0
Date: 27 January 2005
Pagination: i to iii, 1 to 14

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 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. 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 (CSE), 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 CSE, 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.

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) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation 25 January 2005, 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/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Solaris, which is a registered trademark of Sun Microsystems Inc.

TABLE OF CONTENTS

Disclaimer i

Foreword ii

Executive Summary 1

1 Identification of Target of Evaluation 3

2 TOE Description 3

3 Evaluated Security Functionality 3

4 Security Target 3

5 Common Criteria Conformance 4

6 Security Policy 4

6.1 AUTHORIZATION 4
6.2 DISCRETIONARY ACCESS CONTROL 4
6.3 AUDITING 4
6.4 OBJECT REUSE 4
6.5 SECURITY MANAGEMENT 5
6.6 ENFORCEMENT 5
6.7 SEPARATION OF DUTIES 5
6.8 HIERARCHICAL PROFILE RIGHTS 5
6.9 ROLES 5

7 Assumptions and Clarification of Scope 5

7.1 SECURE USAGE ASSUMPTIONS 5
7.2 ENVIRONMENTAL ASSUMPTIONS 6
7.3 CLARIFICATION OF SCOPE 6

8 Architectural Information 6

9 Evaluated Configuration 8

10 Documentation 9

11 Evaluation Analysis Activities 9

12 ITS Product Testing 10

12.1 ASSESSING DEVELOPER TESTS 11
12.2 INDEPENDENT FUNCTIONAL TESTING 11

12.3 INDEPENDENT PENETRATION TESTING 11
12.4 CONDUCT OF TESTING 12
12.5 TESTING RESULTS 13
13 Results of the Evaluation 13
14 Evaluator Comments, Observations and Recommendations 13
15 Glossary 14
16 References 14

Executive Summary

Solaris 9 Release 8/03, from Sun Microsystems Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4+ 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 Protection Profiles developed under the Common Criteria standard. (See section 5.) A Solaris 9 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 (TCB).

CGI Information Systems and Management Consultants Inc. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 14 January 2005, 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 9 8/03, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of Solaris 9 8/03 are advised to verify that their own environment is consistent with 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 indicate that it meets the EAL 4+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The augmentation of ALC_FLR.3 - Systematic flaw remediation is claimed.

Solaris 9 8/03 conforms to the Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999 and the Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998.

The Communications Security Establishment, as the CCS Certification Body, declares that the Solaris 9 8/03 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.

---

[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 + evaluation is Solaris 9, Release 8/03, 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 Protection Profiles developed under the Common Criteria standard. A Solaris 9 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 (TCB).

The primary security features of Solaris 9 8/03 are:

a) Authorization
b) Discretionary Access Control;
c) Object Reuse;
d) Identification and Authentication;
e) Roles and Profiles;
f) Security Management;
g) Auditing; and
h) Enforcement.

See section 2.4 in the ST for a more complete detailed description of the TOE.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Solaris 9 8/03 is identified in Section 6.1 of the ST.

4 Security Target

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

Title: Solaris 9 Security Target
Version: 1.0
Date: 21 December 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*, incorporating all final CC interpretations issued prior to August 1, 2003. Solaris 9 8/03 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 compliant, with all the security assurance requirements in the EAL 4 package, augmented with the ALC_FLR.3 assurance component.

Solaris 9 8/03 conforms with the *Controlled Access Protection Profile (CAPP), Version 1.d,October 8, 1999* and the *Role Based Access Control Protection Profile (RBAC PP), Version 1.0, July 30, 1998*.

6 Security Policy

The Solaris 9 8/03 security policy is described in this section.

6.1 Authorization

Solaris 9 8/03 ensures that only authorized users gain access to the TOE and its resources.

6.2 Discretionary Access Control

Solaris 9 8/03 provides its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users.

6.3 Auditing

Solaris 9 8/03 provides the means of recording any security relevant events, so as to:

a) Assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and
b) Hold users accountable for any actions they perform that are relevant to security.

6.4 Object Reuse

Solaris 9 8/03 ensures that any information contained in a protected resource is not released when the resource is recycled.

6.5 Security Management

Solaris 9 8/03 allows administrators to effectively manage the TOE and its security functions, and ensures that only authorized administrators are able to access such functionality.

6.6 Enforcement

The Solaris 9 8/03 security policy is enforced in a manner, which ensures that the organizational policies are enforced in the targeted environment (i.e., the integrity of the TSF is protected).

6.7 Separation of Duties

Solaris 9 8/03 provides the capability of enforcing the separation of duties, so that no single user is required to perform all administrative functions.

6.8 Hierarchical Profile Rights

Solaris 9 8/03 allows hierarchical definitions of profile rights. The hierarchical definition of rights gives the ability to define profile rights in terms of other profile rights.

6.9 Roles

Solaris 9 8/03 prevents users from gaining access to and performing operations on its resources and objects unless they have been granted access by the resource or objects owner or have been assigned a rights profile or role which permits those operations.

7 Assumptions and Clarification of Scope

Consumers of Solaris 9 8/03 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 9 8/03.

7.1 Secure Usage Assumptions

The following secure usage assumptions, which are consistent with the ST, have been made during the evaluation of Solaris 9 8/03:

a) Each individual user has a unique user ID;
b) Those responsible for the TOE must configure minimum password length for normal users to be at least 8 characters; and

c) If the product comprises more than one platform, then all platforms are administered from a central point within each LDAP directory domain.

7.2 Environmental Assumptions

The following environmental assumptions, which are consistent with the ST, have been made during the evaluation of Solaris 9 8/03:

a) 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) There are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile; and
c) All bridges and routers are assumed to correctly pass data without modification.

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, 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.

8 Architectural Information

The TOE comprises of the following subsystems:

a) Kernel;
b) File System;
c) Audit;
d) I&A;
e) LDAP;
f) Trusted Startup; and
g) Trusted Admin Tools.

The Kernel of Solaris has two primary inter-process communication mechanisms:

a) Networking, providing both *inter*- and *intra*-machine communication paths; and
b) System V Inter- Process Communications (SVIPC), which provides only *intra*-machine paths.

The SVIPC package consists of three mechanisms:

a) Semaphores;
b) Message Queues; and
c) 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 between themselves.

The File system component provides a system call interface, which is used to access and modify information stored on a variety of different file system types. The system call interface provides a consistent set of operations, which can be performed on all the file system types, which simplifies the implementation of the subjects that interact with the file system.

The Audit subsystem provides a record of events that may be used to assign responsibility to actions taking place on a Solaris system. Auditing allows the actions of individual users to be reconstructed and the nature of their activities to be assessed. Individuals can be monitored for attempts to compromise the security of the Solaris system. In addition the extent that the system has been penetrated can be determined.

The I&A subsystem allows users to login to Solaris. The primary method of logging into Solaris is based on the CDE Login Manager *dtlogin*. The *dtlogin* program provides services similar to those provided by *init*, *getty*, and *login* on character terminals. Solaris also allows login from terminal devices and remotely over a network.

The LDAP subsystem maintains a central database of name services information for workstations and servers within a Domain. In the evaluated configuration, there must be a system running a Directory Server master containing the stored databases, and a client workstation.

At any given time, the Solaris operating system is said to be operating in a specific configuration, also known as the system run level. The run level determines what state the system is in, and what system services are available to the users. The *init* command is used to transition the operating system from one run level to another. At any given time, a number of system services are available to the users. What services are available is dependent on the run level at which the system is running. System start-up can be viewed as a run level transition from run level 0 to the system default run level.

The Trusted Admin Tools include the following tools:

a) File Manager – it is a desktop application that enables users to create, locate, organize and work with files and directories on the desktop; and

b) Solaris Management Console (SMC) – it provides Solaris with a Graphical User Interface (GUI) where a set of tools is provided in order to help in administering a distributed Solaris system.

9 Evaluated Configuration

The target of evaluation was evaluated on the following platforms:

a) Platform 1: Entry Level workstations and servers utilizing an UltraSPARC III, UltraSPARCIIIi or UltraSPARCIIi processor in a single or multiple configuration. Various configurations of these platforms are possible and the evaluation scope includes all possible combinations/permutations. An Impact Analysis and Rationale Report shows platform equivalency across the SunFire midframe family. The possibilities are listed in Tables 1, 2 and 3 below of the ST; and

b) Platform 2: The SunFire mid-frame and high-end family offering Dynamic Reconfiguration and Multiple Domaining as defined in Section 1.5. Various configurations of these platforms are possible and the evaluation scope includes all possible combinations/permutations. An Impact Analysis and Rationale Report shows platform equivalency across the SunFire midframe family. The possibilities are listed in Table 4 of the ST.

Please refer to Appendix A of the ST for tables illustrating the hardware configurations available for use. Note that within each platform group, the processor speed associated with each model is dependant upon what was or is offered by the vendor.

The evaluated configurations are defined as follows:

a) When installing the product, the entire distribution should be selected;

b) No additional SMC add-ons should be installed;

c) Minimum physical memory and disk configurations required for the hardware referred above are provided with the Solaris 9 08/03 documentation and may not be sufficient for all applications. For components which must be installed separately from the Solaris Installation, please consult that component's installation guide to determine requirements;

d) The CDE windowing environment must be used in preference to OpenWindows;

e) Solaris 9 supports the use of IPv4 and IPv6, however IPv6 is not part of the TOE;

f) Support for DHCP is not included;

g) 64 bit architectures are included;

h) Web Based Enterprise Management Services (WBEM) are not included;

i) Network, Web Start, Jumpstart, Flash, DVD and CD installations are all supported;

j) The default configuration for identification and authentication only. Support for other authentication options (e.g., smart card authentication) is not included in the evaluated configuration;

k) If the system console is used, it must be connected directly to the server/workstation and afforded the same physical protection as the server/workstation;
l) The evaluated configuration may include the optional installation and deployment of the Sun Java System Application Server version 7.1 (SJAS). No additional security claims are made for SJAS;
m) The product comprises one or more of the above listed servers and/or workstations (and optional peripherals) running the above listed system software (a platform running the above listed software is referred to as a "TOE platform" below);
n) If the product is configured with more than one TOE platform, they are linked by Ethernet LANs, which may be joined by bridges/routers or by TOE platforms which act as routers/gateways; and
o) No other processors may be connected to the Ethernet network, except as noted below.

10 Documentation

The documentation for Solaris 9 8/03 consists of the following:

a) The Release Notes;
b) The Security Release Notes;
c) The Delivery and Configuration Procedures;
d) The System Administration Guide: Basic Administration;
e) The System Administration Guide: Advanced Administration;
f) The System Administration Guide: Security Services;
g) The Common Desktop Environment: User's Transition Guide;
h) The Common Desktop Environment: User's Guide;
i) The Common Desktop Environment: Advanced User's Guide;
j) The Common Desktop Environment: Advanced User's and System Administrator's Guide; and
k) The man pages.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Solaris 9 8/03, including the following areas:

Configuration management: An analysis of the Solaris 9 8/03 development environment and associated documentation was performed. The evaluator found that Solaris 9 8/03 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and 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 9 8/03 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 9 8/03 functional specification and high-level design; 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 9 8/03 user and administrator 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 assessed 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 9 8/03 design and implementation. The evaluators have also determined that the developer has established flaw remediation procedures that sufficiently describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Finally, the evaluators have 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.

Vulnerability assessment: The Solaris 9 8/03 ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability, misuse and strength of function analyses. In addition, the evaluators performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in Solaris 9 8/03.

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 in terms of coverage and depth, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The developers' tests comprise a Test Suite, which contains 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 quite a few test cases, which include test procedure descriptions and expected test results.

The evaluators found the Test Suite gave a complete coverage of the Functional Specification and a complete coverage of the TSF. The Test Suite also demonstrated a satisfactory depth of coverage for all of the High Level Design subsystems.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests that were taken from three sources:

a) The Solaris 9 8/03 Automated Test Suite;
b) The Solaris 9 8/03 Developers Manual Tests; and
c) The Solaris 9 8/08 Security Testing – Installation procedure.

In order to gain assurance in the developer's testing effort, the focus of the independent testing was on execution of a large subset of the developer's tests (i.e., the complete Automated Test Suite was reran and selected ad hoc manual tests were also reran). In order to gain assurance that the TSF operates in accordance with its functional specification on all certified hardware platforms, a subset of tests was conducted on every platform.

During this evaluation, the evaluators also created and executed additional test cases that augmented the developer's tests.

12.3 Independent Penetration Testing

During this evaluation, the evaluator developed independent penetration tests that were taken from four sources:

a) The Solaris 9 8/03 Automated Test Suite;
b) The Solaris 9 8/03 Developers Manual Tests;
c) The Solaris 9 8/08 Security Testing – Installation procedure; and
d) Public sources.

Sun monitors public sources and hacker sites looking for vulnerabilities and exploits. This information is fed to the incident response teams and gives rise to appropriate Bugtraq entries. The public sources consulted include the following:

a) www.securityfocus.com;
b) www.secunia.com;
c) www.sunsolve.com;
d) www.insecure.org;
e) www.securitytracker.com; and
f) www.cert.org.

The evaluators assessed Sun's knowledge of vulnerabilities in the TOE gained from the above sources in producing the vulnerability analysis and thus the evaluators consider that the developer's search for vulnerabilities has considered all relevant information, including the design and implementation.

The approach used in conducting the penetration test cases consisted of satisfying several key objectives:

a) Verification that the certification patch set was effective in mitigating vulnerabilities known to exist in Solaris 9 8/03;
b) Attempts to disprove the developers vulnerability analysis;
c) Regression, involving re-running penetration tests from the previous certification; and
d) Independent penetration testing based on a flaw hypothesis conducted by the evaluator.

12.4 Conduct of Testing

Solaris 9 8/03 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, located in *Ottawa, Ontario*. 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 the Evaluation Technical Report (ETR)[2].

[2] 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Solaris 9 8/03 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 9 8/03 in its intended operating environment

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4+** level of assurance, including the augmentations identified in Section 5 of this report. 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 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

Acronym/Abbreviation/Initialization	Description
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
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

16 References

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

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999;

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999;

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002;

d) Security Target for Solaris 9 8/03 (EAL4+), Version 1.0, 21 December 2004; and

e) Evaluation Technical Report of Solaris 9 8/03, Version 1.0, 14 January 2005.