Certification Report

EAL3+ Evaluation of CA Directory r12.0 SP3

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2011

Evaluation number:	383-4-167-CR
Version:	1.0
Date:	1 March 2011
Pagination:	i to iii, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has 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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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/IEC 17025:2005, General requirements for the Competence of Testing and Calibration 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 EWA-Canada located in Ottawa, Canada.

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 1 March 2011, 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 (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following registered trademarks:

- Oracle is a registered trademark of Oracle Corporation; and
- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

CA Directory r12.0 SP3 (hereafter referred to as CA Directory), from CA, Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

CA Directory is a Directory software application that provides access control over electronic data. CA Directory comprises the components: Directory Server; DXtools, and DXconsole. Administrators initialize and configure the Directory Server using DXtools. Once initialized, Administrators manage the Directory Server using DXconsole. CA Directory can be deployed as a standalone Directory, a replicated Directory for high availability, or as a distributed Directory. User data is stored in an external repository. CA Directory uses the X.501[1] access control scheme to control access to its repository data.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 1 February 2011 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 the CA Directory, 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 (ETR)[2] for this product provide sufficient evidence that it meets the EAL 3 Augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the CA Directory 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

[1] X.500 Series Standard for Electronic Directories including DAP, DSP, DISP, DOP

[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.

Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is CA Directory r12.0 SP3 (hereafter referred to as CA Directory), from CA, Incorporated.

2 TOE Description

CA Directory is a Directory software application that provides access control over electronic data. CA Directory comprises the components: Directory Server; DXtools, and DXconsole. Administrators initialize and configure the Directory Server using DXtools. Once initialized, Administrators manage the Directory Server using DXconsole. CA Directory can be deployed as a standalone Directory, a replicated Directory for high availability, or as a distributed Directory. User data is stored in an external repository. CA Directory uses the X.501[3] access control scheme to control access to its repository data.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for CA Directory is identified in Section 2.5 of the Security Target (ST).

4 Security Target

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

Title: CA Directory r12.0 SP3 Security Target for EAL3+
Version: 3.0
Date: 30 November 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

CA Directory is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only on functional components in Part 2;

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only on assurance components in Part 3; and

[3] X.500 Series Standard for Electronic Directories including DAP, DSP, DISP, DOP

c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.1– Basic Flaw Remediation.

6 Security Policy

CA Directory implements the X.501 access control scheme to control user access to its repository data. In addition, CA Directory implements policies pertaining to Security Audit, Data Protection, Identification and Authentication, Security Management, and High Availability. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of CA Directory should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- The TOE will be managed by one or more competent individuals who are not careless, hostile, or willfully negligent and who will follow and abide by guidance documentation.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

7.3 Clarification of Scope

CA Directory is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration for CA Directory comprises CA Directory r12.0 SP3 Build 4346 running on Oracle Solaris 10 and on Windows Server 2003 SP2.

9 Documentation

The CA documents provided to the consumer are as follows:

a. CA Directory Administration Guide for r12.0;

b. CA Directory Installation Guide for r12.0;

c. CA Directory Reference Guide for r12.0; and

d. CA Directory Release Summary for r12.0.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the CA Directory, including the following areas:

Development: The evaluators analyzed the CA Directory functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the CA Directory security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the CA Directory preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the CA Directory configuration management system and associated documentation was performed. The evaluators found that the CA Directory configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluator examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the CA Directory design and implementation. The evaluator confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluator examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of CA Directory during distribution to the consumer.

The evaluator reviewed the flaw remediation procedures used for CA Directory. During a site visit, the evaluator examined the evidence generated by adherence to the procedures. The evaluator concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of CA Directory. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables.

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

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developers have met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[4].

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 and TOE design was complete.

11.2 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 EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

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

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests; and

c. Independent Evaluator Testing: The objective of this test goal is to augment developer testing of DXconsole commands.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. Penetration testing focused on the effects of communications disconnects on TOE operation.

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

11.4 Conduct of Testing

CA Directory was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. Testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada and at the CA, Incorporated site. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Procedures and Test Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that CA Directory behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the CA Directory includes comprehensive Evaluation, Installation, and User Guides.

The CA Directory is straightforward to configure, use and integrate into a corporate network.

The developer has an extensive and robust automated test suite capable of insuring a proper working product.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
DAP	Directory Access Protocol
DISP	Directory Information Shadowing Protocol
DOP	Directory Operational binding management Protocol
DSP	Directory System Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
X.500	International Standard for Electronic Directories including DAP, DSP, DISP, DOP

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. CA Directory r12.0 SP3 Security Target for EAL3+, Version 3.0, 30 November 2010.

e. Evaluation Technical Report (ETR) for EAL3+ Common Criteria Evaluation of CA Directory r12.0 SP3 , Document No. 1664-000-D002, Version 1.2, 1 February 2011, Common Criteria Evaluation Number: 383-4-167.