Certification Report

EAL 2+ Evaluation of Data Domain Operating System v4.8.2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-135-CR
Version: 1.0
Date: 24 November 2010
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 CEM CC version e.g. *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. 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, the 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, 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 24 November 2010, 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 and the Common Criteria Portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

Explanatory Note:

Data Domain, Inc. was acquired by EMC Corporation ("EMC") in July 2009, and converted to Data Domain LLC, a Delaware limited liability company, effective as of December 21, 2009. Data Domain LLC ("Data Domain") is a direct or indirect wholly owned subsidiary of EMC Corporation.

Data Domain Operating System v4.8.2.0 (hereafter referred to as DD OS), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

DD OS disk-based de-duplication storage systems optimize data protection and disaster recovery performance. DD OS supports all leading enterprise backup and archive applications for integration into existing Information Technology (IT) infrastructures. The integrity of stored data is ensured via multiple levels of data checking and repair.

The primary benefit of an EMC Data Domain solution is the DD OS data de-duplication technology, which stores only unique "segments" of files on disk, significantly reducing the amount of physical storage required in a typical backup environment. Data de-duplication technology can be performed on-the-fly at line-speed.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 2 November 2010 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 DD OS, 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)[1] for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the

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

evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the DD OS 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation is the Data Domain Operating System v4.8.2.0 (hereafter referred to as DD OS), from EMC Corporation.

2 TOE Description

DD OS disk-based de-duplication storage systems optimize data protection and disaster recovery performance. DD OS supports all leading enterprise backup and archive applications for integration into existing Information Technology (IT) infrastructures. The integrity of stored data is ensured via multiple levels of data checking and repair.

The primary benefit of an EMC Data Domain solution is the DD OS data de-duplication technology, which stores only unique "segments" of files on disk, significantly reducing the amount of physical storage required in a typical backup environment. Data de-duplication technology can be performed on-the-fly at line-speed.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DD OS is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: EMC Corporation Data Domain Operating System v4.8.2.0 Security Target
Version: 0.7
Date: 18 October 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

DD OS is:

a. Common Criteria Part 2 extended, with security functional requirements based only upon functional components in Part 2 except for the following explicitly stated requirements defined in the ST:
    - EXT_FDD_DDR.1, Duplicate Data Removal
    - EXT_FRU_RLP.1, Minimum and Maximum retention lock periods

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 augmented, with all security the assurance requirements in the EAL 2 package as well as the following: ALC_FLR.2 – Flaw reporting procedures.

6 Security Policy

DD OS implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information accessed by external server system; details of these security policies can be found in Section 5 of the ST.

In addition, DD OS implements other policies pertaining to security audit, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of DD OS 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 Assumptions are listed in the ST:

- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security will be provided for the TOE and its environment.
- The IT environment provides the TOE with the necessary reliable timestamps.

7.3 Clarification of Scope

The DD OS is intended for use by a non-hostile and well-managed user community. It relies on the environment to provide physical protection and to provide secure communications between systems connected to the TOE.

8 Evaluated Configuration

The evaluated configuration for DD OS comprises: Data Domain Operating System v4.8.2.0 Build 201150. The TOE encompasses the entire DD OS software image and excludes the hardware on which the DD OS executes. The EMC Data Domain appliance hardware models are specified in section 1 of the ST.

The DD OS requires the following components to be properly configured and available in the operational environment:

- EMC Data Domain appliance hardware, on which the DD OS runs, including local storage for de-duplicated backup data;
- Management Workstation, used to administer the DD OS;
- Backup Server(s), which use the DD OS for storage and retrieval of backup data;
- Optional external authentication server; and
- Optional Storage Area Network (SAN), in which the DD OS can store and retrieve de-duplicated backup data.

The publication entitled Data Domain Installation and Setup Guide, 761-0012-0003 Revision A, 2009 contains instructions for installing this system in the evaluated configuration.

9 Documentation

The EMC Corporation documents provided to the consumer are as follows:

- DD OS 4.8 Administration Guide, 759-0003-0001 Revision A, November 20, 2009;
- Data Domain Installation and Setup Guide, 761-0012-0003 Revision A, 2009;
- Data Domain Operating System Release Notes Version 4.8.2.0-201150 Secure Delivery Document;
- Initial Configuration Guide, 761-0022-0001 Revision A, November 2, 2009;

- Command Reference Guide, 762-0006-0001 Revision A, November 2, 2009; and
- Data Domain Operating System 4.8.2.0 Guidance Documentation Supplement, 0.3, August 31, 2010.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DD OS, including the following areas:

Development: The evaluators analyzed the DD OS 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 DD OS security architectural description and determined that the initialization process is secure, 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 DD OS preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes 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 DD OS configuration management system and associated documentation was performed. The evaluators found that the DD OS configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of DD OS during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by EMC for DD OS. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators 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 DD OS. Additionally, the evaluators conducted a search of public domain vulnerability

databases to identify DD OS potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the DD OS in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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 developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification 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. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

c. Security Management: The objective of this test goal is to ensure the users and roles functionality is correct;

[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.

d. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met; and

e. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed.

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.

The penetration tests focused on:

Port Scanning: The objective of this test goal is to determine if the Management workstation opens any ports that could be exploited from the network;

Leakage verification: The objective of this test goal it to monitor the TOE for data loss during start up and shut down; and

Misuse: The objective of this test goal is to test the TOE for misuse by SQL injection.

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

11.4 Conduct of Testing

DD OS was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that DD OS behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 + 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

EMC demonstrated a very strong commitment to ensuring the security of their product. A project manager and a team of software engineers dealt exclusively with security issues and interacted with the other teams regularly. This team makes all security-related decisions and ensures that either they or the appropriate functional team address any issues.

The evaluators would like to commend EMC on their life cycle processes and tools used to support them. We were particularly impressed with the variety of tools and the integration of them that allows EMC to provide detailed tracking of development, bug resolution and delivery of product and updates to their customers.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System
CPL	Certified Products list
DD OS	Data Domain Operating System
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
SAN	Storage Area Network
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	Toe Security Functionality
TSFI	TOE security functionality Interfaces

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. CC version e.g. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. CEM version e.g. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. EMC Corporation Data Domain Operating System v4.8.2.0 Security Target, v0.7, 18 October 2010

e. Evaluation Technical Report for EAL2+ Common Criteria Evaluation of Data Domain Operating System v4.8.2.0, Version 1.2, 2 November 2010