Certification Report

EAL 2+ Evaluation of RSA® Data Loss Prevention Suite v9.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-219-CR
Version: 1.0
Date: 15 October 2012
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, 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 15 October 2012, 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 trademark:

- RSA® is a registered trademark of RSA, The Security Division of EMC

TABLE OF CONTENTS

Executive Summary

RSA® Data Loss Prevention Suite v9.0 (hereafter referred to as DLP Suite), from RSA, The Security Division of EMC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

DLP Suite allows an enterprise to identify sensitive information in text format stored on its computers, and as it is being transmitted between IT entities or being copied, saved, or printed. The TOE then takes actions based on pre-defined policies to protect the information from loss and misuse. There are four components within DLP Suite that provide this functionality: DLP Enterprise Manager, DLP Datacenter, DLP Network, and DLP Endpoint. The DLP Datacenter, DLP Network, and DLP Endpoint are managed through the DLP Enterprise Manager, a web application with a consistent user interface across all the products.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 17 September 2012 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 DLP Suite, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 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 DLP Suite 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 ETR 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) 2 augmented evaluation is RSA® Data Loss Prevention Suite v9.0 (hereafter referred to as DLP Suite), from RSA, The Security Division of EMC.

2 TOE Description

The DLP Suite is an integrated suite of software products which run on RSA appliances or customer-provided hardware. DLP Suite allows an enterprise to identify sensitive information in text format stored on its computers and as it is being transmitted between IT entities or being copied, cut, moved, saved or printed. The DLP Suite takes actions based on pre-defined policies to determine whether the action being taken on the information should be permitted. An *allow* action causes the attempted end-user action to be permitted. An *audit* action generates an event describing the violation. A *quarantine* action forces access to the sensitive content to be restricted to a designated end-user or group. A *block* action disallows the attempted violation. A *notify* action causes a notification of the violation to be sent to the end-user who committed it. A *justify* action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action. Each policy action taken is captured in an event record, and passed to the DLP Enterprise Manager for viewing by the administrator. The DLP Suite also generates “incidents”, which are higher-level issues that require manual remediation by an administrator.

There are four components within the DLP Suite briefly described as follows:

- The DLP Datacenter product provides the ability to identify sensitive content stored on laptops, desktops, and servers distributed through a corporate environment;
- The DLP Network product detects sensitive data while it is being transmitted across the network, and generates events and incidents reflecting policy violations;
- The DLP Endpoint product provides control over sensitive information being manipulated by end-users; and
- The DLP Enterprise Manager is a web application with a consistent user interface which is used to manage the DLP Datacenter, DLP Network and DLP Endpoint products.

A detailed description of the DLP Suite architecture is found in Section 1.3 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DLP Suite is identified in Section 6 of the ST.

4 Security Target

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

Title: RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v9.0
Version: 0.7
Date: 17 September 2012

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.*

DLP Suite is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - EXT_FIH_ARP.1 Incident Alarms; and
   - EXT_FIH_SAA.1 Incident Analysis
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*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

DLP Suite implements an access control policy for administrators accessing the TOE and end-user access control polices which enforce rules governing the ability of end-users to take actions on data. The TOE also implements an information flow control policy which enforces rules governing the ability of end-users to transmit sensitive data across or out of the network. Details of these security policies can be found in Section 6 of the ST.

In addition, the DLP Suite implements policies pertaining to security audit, identification and authentication, security management, TOE access and incident handling. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of DLP Suite 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:

- Authorized administrators who manage the TOE and systems in the IT Environment are non-hostile and are appropriately trained to use, configure, and maintain the TOE, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE, along with all TSF-dependent services, including the LDAP server with which the TOE interfaces, reside in a physically controlled access facility that prevents unauthorized physical access.

- The IT environment provides a secure line of communication between distributed portions of the TOE and between the TOE and remote administrators.

7.3 Clarification of Scope

DLP Suite offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. DLP Suite is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

A policy rule which can be selected by an administrator is "tag for encryption" which will encrypt emails containing sensitive information. For the purposes of this evaluation the term "tag for encryption" represents a rule selector and not the action of encryption. Encryption, if selected and available, is performed by a third-party product, and is outside the scope of this evaluation.

8 Evaluated Configuration

The evaluated configuration for DLP Suite comprises the following software components:

- DLP Enterprise Manager version 9.0.0.10051;

- DLP Datacenter Enterprise Coordinator version 9.0.0.10041;
- DLP Network Controller version 9.0.0.10027;
- DLP Network Sensor version 9.0.0.10027;
- DLP Network Interceptor version 9.0.0.10027;
- DLP Network ICAP Server version 9.0.0.10027;
- DLP Network Exchange Transport Agent version 9.0.0.10027;
- DLP Endpoint Site Coordinator version 9.0.0.10041;
- DLP Endpoint Agent version 9.0.0.10041;
- DLP Datacenter Site Coordinator version 9.0.0.10041;
- DLP Datacenter Agent version 9.0.0.10041; and
- DLP Datacenter Grid Worker version 9.0.0.10041.

Table 2 in the ST lists the minimum hardware and software requirements for the TOE in the CC evaluated configuration.

The publication entitled *RSA Data Loss Prevention Suite v9.0 Guidance Supplement, Document Version 0.1* describes the procedures necessary to install and operate DLP Suite in its evaluated configuration.

9 Documentation

The RSA, The Security Division of EMC documents provided to the consumer are as follows:

a. RSA DLP Network 9.0 User Guide

b. RSA DLP Network 9.0 Deployment Guide

c. RSA DLP Datacenter 9.0 User Guide

d. RSA DLP Datacenter 9.0 Deployment Guide

e. RSA DLP Endpoint 9.0 User Guide

f. RSA DLP Endpoint 9.0 Deployment Guide

g. RSA DLP 9.0 Release Notes

h. RSA Data Loss Prevention Suite v9.0 Guidance Supplement, Document Version 0.1

i. Deploying RSA DLP in FIPS-Compliant Mode Technical Note

j. Guide to RSA DLP for Internal Email Technical Note

k. Configuring Active Directory RMS for use with RSA DLP Technical Note.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DLP Suite, including the following areas:

Development: The evaluators analyzed the DLP Suite 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 DLP Suite 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 DLP Suite 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 DLP Suite configuration management system and associated documentation was performed. The evaluators found that the DLP Suite 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 DLP Suite during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by RSA, The Security Division of EMC for DLP Suite. 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 DLP Suite. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify DLP Suite potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to DLP Suite 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 is 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. Endpoint template blade policy: The objective of this test goal is to verify that an Endpoint Agent can enforce a policy that uses a template blade and stop sensitive documents from being copied, saved or printed;

[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.

c. Datacenter audit scan for sensitive content: The objective of this test goal is to verify that an Enterprise Manager can initiate a Datacenter Agent to scan its local files and report on any sensitive content that may be stored;

d. Endpoint policy with dictionary terms: The objective of this test goal is to verify that an Endpoint Agent can enforce a policy using a custom dictionary on sensitive documents being transmitted; and

e. Agent protection: The objective of this test goal is to verify that users cannot disable Endpoint Agent services from running on their PC.

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:

a. Port Scanning: The objective of this test goal was to scan the TOE using a port scanner to determine what ports were open and what services were running;

b. Information Leakage Verification: The objective of this goal was to verify that the TOE does not reveal sensitive information during system boot up, system shutdown, login to the Enterprise Manager console and Agent host; and

c. Temporarily disable Endpoint Agent: The objective of this test goal was to verify that the code used to temporarily disable an Endpoint Agent cannot be re-used. This test verified that the codes are unique and time limited.

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

11.4 Conduct of Testing

DLP Suite 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 DLP Suite 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

The RSA Data Loss Prevention Suite v9.0 ships with a complete and comprehensive set of user guidance documentation.

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
CM	Configuration Management
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
PC	Personal Computer
ST	Security Target
TOE	Target of Evaluation

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. RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v9.0 Security Target version 0.7, 17 September 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v9.0, version 1.2, 17 September 2012.