Certification Report

EAL 2+ Evaluation of RSA® Data Loss Prevention Suite v6.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-99-CR
Version: 1.0
Date: 12 May 2009
Pagination: i to iii, 1 to 12

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 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 12 May 2009, 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/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked name:

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

TABLE OF CONTENTS

Executive Summary

The RSA® Data Loss Prevention Suite v6.5 (hereafter referred to as DLP Suite), from RSA, The Security Division of EMC, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The DLP Suite helps uncover an organization's risk associated with sensitive data loss and lowers that risk through policy based remediation and enforcement mechanisms. The DLP Suite is an integrated suite of products which 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. There are four products within the DLP Suite: DLP Datacenter, DLP Network, DLP Endpoint and the DLP Enterprise Manager. The DLP Suite takes actions based on pre-defined policies to determine whether the action being taken on the information should be permitted. 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.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 04 May 2009 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 DLP Suite, 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 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:

a. ALC_FLR.1 – Basic Flaw remediation.

[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.

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 in the field of IT Security* 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 augmented evaluation is the RSA® Data Loss Prevention Suite v6.5 (hereafter referred to as DLP Suite), from RSA, The Security Division of EMC.

2 TOE Description

The DLP Suite is an integrated suite of products which 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 products 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.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the DLP Suite is identified in Sections 5 and 6 of the Security Target (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 v6.5 Security Target
Version: 0.7
Date: 20 April 2009

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*.

The 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)
   - 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*, with all the security assurance requirements in the EAL 2 package, as well as ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

The 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 the 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 are the assumptions about the secure usage of the TOE:

- Personnel authorized to install, configure, and operate the DLP Suite possess appropriate training and will adhere to the procedures for secure usage of the product described in the ST and all user guidance.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the TOE:

- The host machine upon which DLP Suite is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.
- It is assumed that the IT environment will provide a secure line of communication between distributed parts of the TOE.

7.3 Clarification of Scope

The DLP Suite provides a level of protection that is appropriate against obvious vulnerabilities in IT environments that require that information flows be controlled and restricted among network nodes and where the DLP Suite can be appropriately protected from physical attack.

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 Architectural Information

The DLP Suite consists of four products that cover the three areas of potential data loss; data moving as network traffic, at rest in a data center, or out at an endpoint. Each product consists of the following components briefly described below.

The DLP Network product consists of the following software and hardware components:

- *DLP Network Controller* is the appliance that maintains information about sensitive data and content transmission policies.
- *DLP Network Sensor* passively monitors traffic crossing the network boundaries and analyzes it for the presence of sensitive content.
- *DLP Network Interceptor* allows administrators to implement policies that quarantine or reject email traffic that contains sensitive content.

- *DLP Network ICAP Server* allows administrators to implement monitoring or blocking of HTTP, HTTPS or FTP traffic containing sensitive content.

The DLP Endpoint product consists of the following software components:

- *DLP Endpoint Enterprise Coordinator* manages the policies and the collection of events from the DLP Endpoint Site Coordinator throughout the network and passes the information to the DLP Enterprise Manager for display in the Graphical User Interface (GUI).
- *DLP Endpoint Site Coordinator* provides services that manage scans for a local network.
- *DLP Endpoint Agent* enforces policies on usage of data, resulting in blockages, justifications, or notifications and generates events that describe the violations and the actions taken to enforce the policies.

The DLP Datacenter product consists of the following software components:

- *DLP Datacenter Enterprise Coordinator* provides instructions and gathers scan results from all DLP Datacenter Site Coordinators installed in the enterprise.
- *DLP Datacenter Site Coordinator* provides services that manage scans for a local network.
- *DLP Datacenter Grid Worker* retrieves and analyzes data from large storage repositories.
- *DLP Datacenter Agent* performs the analysis of data on the designated machines.

The DLP Enterprise Manager is a stand-alone component that comprises the DLP Enterprise Manager software. The DLP Enterprise Manager enables an administrator to configure and manage the DLP Network, Endpoint and Datacenter products.

9 Evaluated Configuration

The TOE runs on RSA appliances or customer-provided hardware compliant to the minimum software and hardware requirements as listed in the Security Target, Table 2 of Section 1.3.7 TOE Environment.

The essential software components for the proper operation of the TOE in the evaluated configuration are:

- DLP Enterprise Manager v6.5.0.2179 software
- DLP Network Controller v6.5.0.2164 software

- DLP Network Sensor v6.5.0.2164 software
- DLP Network Interceptor v6.5.0.2164 software
- DLP Network ICAP Server v6.5.0.2164 software
- DLP Endpoint Enterprise Coordinator v6.5.0.86 software
- DLP Endpoint Site Coordinator v6.5.0.86 software
- DLP Endpoint Agent v6.5.0.86 software
- DLP Datacenter Enterprise Coordinator v6.5.0.86 software
- DLP Datacenter Site Coordinator v6.5.0.86 software
- DLP Datacenter Agent v6.5.0.86 software
- DLP Datacenter Grid Worker v6.5.0.86 software

The essential physical components for the proper operation of the TOE which are outside the TOE boundary and were not evaluated are:

- DLP Network appliances running TabOS based on CentOS v5.1
- Customer-provided hardware for DLP Endpoint and DLP Datacenter running Microsoft Windows 2003 Server or Vista
- Microsoft Internet Explorer 6 web browser installed on the Enterprise Manager
- Targeted customer workstations, servers, and laptops on which DLP Endpoint Agents, DLP Datacenter Agents, and DLP Datacenter Grid Workers will be installed running Microsoft Windows 2003 Server or Vista
- A Microsoft SQL Server 2005 Database to serve as the Enterprise Results Database

10 Documentation

The RSA documents provided to the consumer are as follows:

- RSA DLP Network 6.5 User Guide, 08 December 2008
- RSA DLP Network 6.5 Deployment Guide, 08 December 2008
- RSA DLP Datacenter 6.5 User Guide, 08 December 2008
- RSA DLP Datacenter 6.5 Deployment Guide, 08 December 2008
- RSA DLP Endpoint 6.5 User Guide, 08 December 2008
- RSA DLP Endpoint 6.5 Deployment Guide, 08 December 2008
- RSA, The Security Division of EMC Data Loss Prevention Suite v6.5 Guidance Supplement, Document Version 0.2, 10 February 2009

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the 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 were correct.

Guidance documents: The evaluators examined the DLP Suite 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 were 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 and uniquely 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 the DLP Suite during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by RSA for the 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 the DLP Suite in its operational environment.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessing Developer Tests

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

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.

RSA employs a rigorous testing process that tests the changes and fixes in each release of the DLP Suite. Comprehensive regression testing is conducted for all releases.

12.2 Independent Functional Testing

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

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is 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;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests to gain assurance in the developers testing process;

c. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect data from loss and misuse in accordance with administrator pre-defined polices;

d. Identification and Authentication: The objective of this test goal is to confirm that TOE administrators are identified and authenticated prior to allowing any activity to be performed by them;

e. Security Audit: The objective of this test goal is to ensure that the TOE is capable of generating audit data related to management actions; and

[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.

f. Incident Handling: The objective of this test goal is to ensure that the TOE will generate and deliver alerts to administrators according to configured policies.

12.3 Independent Penetration Testing

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

- Generic vulnerabilities;
- Port scanning;
- Direct attacks to verify the TOE can self-protect itself in its intended environment; and
- Forced exception behaviour of the TOE to verify that an operator of the TOE is prevented from disrupting the proper operation of the TOE through invalid use of processes or configuration parameters.

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

12.4 Conduct of Testing

The 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 Testing (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.

12.5 Testing Results

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

13 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.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the DLP Suite includes comprehensive installation, administration, deployment, and reference guides.

The RSA Quality Assurance facilities were used during a portion of the testing activities. RSA Support was consulted during the initialization of the product in the EWA-Canada ITSET lab.

15 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
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories-Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 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. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

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

d. RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v6.5 Security Target, Revision No. 0.7, 20 April 2009.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v6.5, Document No. 1599-000-D002, Version 1.1, 04 May 2009.