Certification Report

EAL 2+ Evaluation of

Verdasys Digital Guardian v6.0.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-218-CR
Version: 1.0
Date: 25 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 CGI Security Evaluation and Test Facility 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 25 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 trademarks or registered trademarks:

- Digital Guardian is a registered trademark of Verdasys Inc.;
- Verdasys is a trademark of Verdasys Inc; and
- Microsoft and Windows are registered trademarks of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

Verdasys Digital Guardian v6.0.1 (hereafter referred to as Digital Guardian), from Verdasys Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Digital Guardian is a comprehensive Enterprise Information Protection (EIP) solution for workstations and servers evaluated on Microsoft Windows operating systems. EIP solutions secure proprietary and sensitive data while maintaining the integrity of business processes. Digital Guardian offers an enterprise-wide, policy-driven, and data-centric approach to information security.

CGI Security Evaluation and Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 09 October 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 Digital Guardian, 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.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Digital Guardian 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 Verdasys Digital Guardian v6.0.1 (hereafter referred to as Digital Guardian), from Verdasys, Inc.

2 TOE Description

Digital Guardian is a comprehensive Enterprise Information Protection (EIP) solution for workstations and servers evaluated on Microsoft Windows operating systems. EIP solutions secure proprietary and sensitive data while maintaining the integrity of business processes. Digital Guardian offers an enterprise-wide, policy-driven, and data-centric approach to information security.

3 Evaluated Security Functionality

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

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Verdasys Secure Cryptographic Module (VSEC)	1607

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Digital Guardian:

Cryptographic Algorithm	**Standard**	**Certificate #**
Secure Hash Standard (SHS)	FIPS 180-3	1261
Advanced Encryption Standard (AES)	FIPS 197	1384
Rivest Shamir Adleman (RSA)	FIPS 186-2	677
Deterministic Random Bit generators (DRBG)	ANSI X9.82	50
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	814

4 Security Target

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

Title: Verdasys Digital Guardian v6.0.1 Security Target.
Version: 1.4
Date: 2 October 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*.

Digital Guardian 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:
   - ESM_ACD_EXT.1 Access Control Policy Definition;
   - ESM_ACE_XT.1 Access Control Policy Transmission;
   - ESM_DSC_EXT.1 Object Discovery; and
   - ESM_OAD_EXT.1 Object Attribute Definition.

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.2 – Flaw Reporting Procedures.

6 Security Policy

Digital Guardian implements a role-based access control policy to control user access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, Digital Guardian implements policies pertaining to security audit, user data protection, fault tolerance, enterprise information protection and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Digital Guardian 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.
- The authorized administrators are not hostile, are appropriately trained and will follow and abide by the instructions provided by the TOE documentation.

- Subjects acting as end-users of the TOE are authenticated by a secure mechanism.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities.
- Identity and attribute data for TOE agent users is provided by a secure organizational repository in the TOE environment.
- The TOE environment will provide a secure line of communication between the TOE server and agent.

7.3 Clarification of Scope

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

8 Evaluated Configuration

The evaluated configuration for Digital Guardian comprises the following software:

- Verdasys Digital Guardian Server v6.0.1.0042 running on Microsoft Windows 2008 R2.
- Verdasys Digital Guardian Agent v6.0.1.0107 running on Microsoft Windows XP SP3, Server 2003 SP2/R2, or Server 2008 R2.

The publication entitled Guidance Documentation Supplement, version 1.2, 2 October 2012 describes the procedures necessary to install and operate Digital Guardian in its evaluated configuration.

9 Documentation

The Verdasys documents provided to the consumer are as follows:

a. Guidance Documentation Supplement, version 1.2;

b. Installing and Using Digital Guardian Archive and Restore for SQL Server, version 6.0.1;

c. Installing and Upgrading Digital Guardian, version 6.0.1;

d. Quick Reference card, Digital Guardian version 6.0.1;

e. Release Notes – Digital Guardian 6.0.1, Agent build 0107, Server build 0042;

f. Digital Guardian Rule Implementation Guide version 6.0.1;

g. Digital Guardian Unattended Deployment Guide version 6.0.1;

h. Using Digital Guardian version 6.0.1;

i. What's New, Digital Guardian, version 6.0.1, March 30, 2012-10-18;

j. Digital Guardian Server Minimum Requirements v 6.0; and

k. Digital Guardian Utilities version 6.x.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Digital Guardian, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by Verdasys for Digital Guardian. 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 Digital Guardian. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Digital Guardian potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Digital Guardian 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].

[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.

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 CGI Security Evaluation and Test Facility 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. Independent Evaluator testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing: Tests covered in this area include:

- 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;
- Identification and authentication: The objective of this test goal is to show that users with invalid usernames and passwords cannot gain access to the TOE;
- Security Management: the objective of this test goal is to exercise the management of security attributes, functions and roles;
- Network failure: The objective of this test goal is to test the Digital Guardian Agents ability to recover when the network becomes unavailable;
- Vault rules: The objective of this test goal is to demonstrate the use of "vault rules" in developing a common "save-as" protection pattern; and
- Decryption after expiry: The objective of this test goal is to demonstrate that files encrypted with an expired key can have the key retrieved to decrypt those files.

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. Bypassing:

- An attempt was made to bypass the stealth mode so as to identify the Digital Guardian Agent software;
- An attempt was made to subvert enforced policies on the Digital Guardian Agent to allow an attacker to take screen captures of sensitive material and then print those images;
- An attempt was made to bypass the use of blacklisted files;
- An attempt was made to subvert policy by copying data to alternate data streams so as to be able to read it;

b. Privilege Escalation attacks: The objective of this test goal is to attempt to escalate privileges by exploiting one of the "SK" flags; and

c. Avoid Encryption Policies: The objective of this test goal is to attempt to avoid encryption policies by subverting the design by which encryption is applied.

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

11.4 Conduct of Testing

Digital Guardian 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 CGI Security Evaluation and Test Facility. 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 Digital Guardian 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 evaluator noted throughout the testing and vulnerability assessment portion of the evaluation that there are a great deal of configuration options available on the Verdasys Digital Guardian server. The evaluator recommends professional training for any potential administrator on the product and target DG Agent operating system(s) from a qualified training facility.

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
EAL	Evaluation Assurance Level
EIP	Enterprise Information Protection
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TSF	TOE Security Functionality
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. Verdasys Digital Guardian v6.0.1, version 1.4, 02 October 2012 Security Target.

e. Verdasys Digital Guardian v6.0.1, version 1.0, 9 October 2012 ETR.