Certification Report

EAL 4 Evaluation of PGP Desktop: Enterprise Whole Disk Encryption Only Edition, Version 9.10.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-108-CR
Version: 1.0
Date: 27 April 2010
Pagination: i to iv, 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 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 DOMUS IT Security Laboratory 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 27 April 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- ActiveIdentity ActivClientCAC is a trademark of ActivIdentity Corporation;
- Aladdin eToken is a trademark of Aladdin Corporation;
- Athena ASEKey and Athena ASECard are trademarks of Athena Smartcard Solutions;
- Atmel TPM is a trademark of Atmel Corporation;
- Broadcom TPM is a trademark of Broadcom Corporation;
- Charismathics CryptoIdentity is a trademark of Charismathics the middleware company;
- Dell is a trademark of Dell Corporation;

- EMC is a trademark of EMC Corporation;
- Fujitsu LifeBook is a trademarks of Fujitsu Corporation;
- HP and Compaq are trademarks of Hewlett Packard Corporation;
- Infineon TPM is a trademark of Infineon Technologies;
- Lenovo Thinkpad is a trademark of Lenovo Corporation;
- Matsushita BIOS is a trademark of Matsushita Corporation;
- Panasonic Toughbook is a trademark of Panasonic Corporation;
- PGP Universal™ Server is a trademark of PGP Corporation;
- PGP, Pretty Good Privacy and the PGP logo are registered trademarks of PGP Corporation in the US and other countries;
- PGP® Cryptographic Engine is trademark of PGP Corporation;
- PGP® SDK is a trademark of PGP Corporation;
- PGP® Whole Disk Encryption is a trademark of PGP Corporation;
- Phoenix BIOS is a trademark of Phoenix Technologies;
- Rainbow iKey (formerly a trademark of Rainbow) is a trademark of SafeNet;
- RSA and RSA Secure ID are trademarks of RSA Corporation;
- S-Trust StarCOS is a trademark of S-Trust Corporation; and
- Windows is a registered trademark of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

PGP Desktop: Enterprise Whole Disk Encryption Only Edition, Version 9.10.0, Build 596 (hereafter referred to as Managed WDE), from PGP Corporation®, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Managed WDE is a software application that allows users to encrypt their entire hard disk or selected partitions using FIPS 140-2 validated cryptography. Once a disk or partition is encrypted, data (including temporary data) is always written in encrypted form. Managed WDE includes a pre-boot component that replaces the existing Master Boot Record. The pre-boot component requires passphrase, token/smartcard, or Trusted Platform Module authentication to release the keys necessary to decrypt the operating system and data. The "managed" aspect relates to the Managed WDE's ability to be remotely managed using a PGP Universal Server.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 31 March 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 Managed WDE, 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 4 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: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Managed WDE 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) 4 evaluation is PGP Desktop: Enterprise Whole Disk Encryption Only Edition, Version 9.10.0 (hereafter referred to as Managed WDE), from PGP Corporation®.

2 TOE Description

Managed WDE is a software application that allows users to encrypt their entire hard disk or selected partitions using FIPS 140-2 validated cryptography. Once a disk or partition is encrypted, data (including temporary data) is always written in encrypted form. Managed WDE includes a pre-boot component that replaces the existing Master Boot Record. The pre-boot component requires passphrase, token/smartcard, or Trusted Platform Module authentication to release the keys necessary to decrypt the operating system and data. The "managed" aspect relates to the Managed WDE's ability to be remotely managed using a PGP Universal Server.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Managed WDE is identified in Sections 5 and 6 of the Security Target (ST).

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

Cryptographic Module	**Certificate #**
PGP SDK	1101
PGP Cryptographic Engine	*Pending*[2]

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Managed WDE:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	754, 895
Advanced Encryption Standard (AES)	FIPS 197	954, 1253, 1316, 1317
Rivest Shamir Adleman (RSA)	FIPS 186-2	460
Message Digest (SHA-1)	FIPS 180-2	1203
Message Digest (SHA-1,256,384,512)	FIPS 180-2	926, 1149
Random Number Generator	ANSI X9.31	539

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

4 Security Target

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

Title: PGP Desktop: Enterprise Whole Disk Encryption Only Edition Version 9.10.0 Security Target EAL 4 augmented ALC_FLR.1
Version: 1.0
Date: 30 March 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.*

Managed WDE 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:
   - FAU_GEN_EXP.1: Audit Generation – Explicit; and
   - FCS_COP_EXP.1: Cryptographic operation – Recovery Passphrase Generation.

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

c. *Common Criteria EAL 4 augmented,* containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

Managed WDE implements policies pertaining to security audit, user data protection, identification and authentication, 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 TOE short name 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:

- Only a single user is allowed per installed platform, the user is non-hostile, appropriately trained, and follows all user guidance. The Universal Server Administrators that remotely administer the TOE are likewise non-hostile, appropriately trained, and follow provided guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- A PGP Universal Server or Generic Equivalent is provided in the operational environment which supports the review of audit records passed to it by Managed WDE.

- The operational environment shall provide an accurate time source for use in time stamps.

- The PGP Universal Server or its equivalent in the operational environment is physically secure.

- The Operational Environment shall provide an authentication server for use in Managed WDE enrollment to the PGP Universal Server.

- The Operational Environment provides a TPM module, a SmartCard or a Token (as required) and cryptographic keypairs to support secure access to cryptographic keys used to encrypt/decrypt protected resources.

7.3 Clarification of Scope

Managed WDE is designed to protect data physically stored on a hard drive. It protects data while the platform is powered off (i.e. the decryption keys are not stored in volatile memory). Managed WDE authenticates the local user at boot time and does not provide any access control to data while Managed WDE is running.

Protection against network based threats fall outside Managed WDE's intended use and should be addressed by other security mechanisms such as firewalls, anti-virus, and intrusion detections systems.

8 Architectural Information

Managed WDE comprises two main components: the PGP desktop and the mWDE disk BIOS. The PGP desktop engages following the boot process of the local machine and provides the main user GUI management interface. The mWDE disk BIOS engages during powerup providing the interface used to enter the user passphrase or to access a token key.

The mWDE disk BIOS then validates the user credentials and initiates decryption of the encrypted boot disk to allow for system startup.

Further detail on the architecture may be found in Section 1.7 - Architecture Description of the ST.

9 Evaluated Configuration

The evaluated configuration for Managed WDE comprises:

- PGP Desktop: Enterprise Whole Disk Encryption Only Edition, Version 9.10.0 executing on Windows XP Professional SP3.
- PGP Universal Server v2.10.0.
- (optional) Smartcard or Token for authentication:
    - ActiveIdentity ActivClientCAC cards, 2005 models;
    - Aladdin eToken 64K, 2048-bit RSA-capable;
    - Aladdin eToken PRO USB Key 32K, 2048-bit RSA-capable;
    - Aladdin eToken PRO without 2048-bit capability (older smart cards);
    - Athena ASEKey Crypto USB Token for Microsoft ILM;
    - Athena ASECard Crypto Smart Card for Microsoft ILM;
    - EMC RSA SecurID SID800 Token;
    - Charismathics CryptoIdentity plug 'n' crypt Smart Card only stick;
    - S-Trust StarCOS smart card; and
    - Rainbow iKey 3000.
- (optional) TPM for authentication:
    - Hewlett-Packard Compaq nx6325 (Infineon TPM with HP BIOS);
    - Dell D620/D630 (Broadcom TPM);
    - Lenovo ThinkPad T60 (Atmel TPM);
    - Fujitsu LifeBook T2010, (Infineon TPM with Phoenix BIOS); and

- Panasonic Toughbook T5, W5, or Y5 (Infineon TPM with Matsushita BIOS).

The publication entitled Managed Whole Disk Encryption Common Criteria Supplement Version 9.10.0 describes the procedures necessary to install and operate Managed WDE in its evaluated configuration.

10 Documentation

The PGP documents provided to the consumer are as follows:

- PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10.0;
- PGP® Desktop for Windows User's Guide, PGP Desktop Version 9.10.0;
- PGP® Desktop Version 9.10 for Windows Release Notes (version 9.10.0); and
- Managed Whole Disk Encryption Common Criteria Supplement Version 9.10.0.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Managed WDE, including the following areas:

Development: The evaluators analyzed the Managed WDE functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Managed WDE security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Managed WDE 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 Managed WDE configuration management system and associated documentation was performed. The evaluators found that the Managed WDE configuration items were clearly marked and could be modified and controlled by automated tools. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM

plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Managed WDE design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by PGP for Managed WDE. 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 Managed WDE. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the Managed WDE in its operational environment.

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

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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[3].

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

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

test documentation and the functional specification, TOE design and security architecture description was complete.

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 was the following list of DOMUS IT Security Laboratory 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. Cryptographic Support: The objective of this test goal is to verify that cryptographic operations are invoked as described in the TOE design;

c. Protection of the TOE: The objective of this test goal is to determine that the TOE can protect itself from malicious entities and that the TOE does not compromise user data in the event that it is tampered with;

d. Security Management: The objective of this test is to determine the correct operation of the remote interactions with the management server;

e. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data;

f. Audit: The objective of these tests is to ensure that User Access Events Logging requirements have been met; and

g. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of 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 Managed WDE opens any ports that could be exploited from the network; and

- Boot/Network Failures: The objective of this test goal is to determine if partial boots or network connectivity problems cause unexpected behavior.

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

12.4 Conduct of Testing

Managed WDE 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 DOMUS IT Security Laboratory. 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 Managed WDE behaves as specified in its ST, functional specification, TOE design and security architecture description.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 + 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

Consumers are advised to review the security aspects of the intended environment (defined in Sections 3 and 4 of the ST) when deploying the PGP Managed WDE.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
BIOS	Basic Input/Output System
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level

Acronym/Abbreviation/ Initialization	Description
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories - Canada
PIN	Personal Identification Number
RNG	Random Number Generator
SDK	Software Developer's Kit
SFR	Scurity Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE security functionality
WDE	Whole Disk Encryption
WDRT	Whole Disk Recovery Token

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, CEM, Version 3.1 Revision 2, September 2007.

d. PGP Desktop: Enterprise Whole Disk Encryption Only Edition Version 9.10.0 Security Target EAL 4 augmented ALC_FLR.1, Version 1.0, 30 March 2010

e. Evaluation Technical Report, Version 1.6, PGP Desktop: Enterprise Whole Disk Encryption Only Edition Version 9.10.0, EAL 4, 31 March 2010